



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/716,336	11/18/2003	Nicholas Stamos	3602.1000-003	5223

21005 7590 11/26/2007
HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

EXAMINER

LEMMA, SAMSON B

ART UNIT	PAPER NUMBER
----------	--------------

2132

MAIL DATE	DELIVERY MODE
-----------	---------------

11/26/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

mn

Office Action Summary	Application No.	Applicant(s)	
	10/716,336	STAMOS ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 November 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-6, 8-19 and 21-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-6, 8-19 and 21-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The request filed on November 09, 2007 for a request for continued examination (RCE) under 37 CFR 1.114 based on patent application 10/716,336 is acceptable and an RCE has been established.
2. **Claims 7 and 20** are canceled and new dependent **claims 23 and 24** are added. Thus claims **1-6, 8-19 and 21-24** are pending/examined. All the claims except dependent **claims 6 and 19** are amended of which **claims 1 and 17** are independent claims.

Response to Arguments

3. Applicant's arguments filed on November 09, 2007 have been fully considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. **Claims 1-6, 8-19 and 21-24** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Belfiore et al.** (hereinafter referred as **Belfiore**)(U.S. Patent No. 6,990,513 B2) (filed on Jun 22, 2001) in view of Ginter et al Title (hereinafter refereed as **Ginter**) (Patent No. 7,165,174 B1) (filed on December 17,1999)

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as

applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner

5. **As per claims 1 and 16-17 and 23-24 Belfiore discloses a system for providing a usage accountability model for data security in a data processing system comprising:**

- **A user device having a sensor for to sense or capture atomic level events at a point of authorized access to at least one digital asset by an end user client device;** *[column 20, lines 57-58, figure 5, ref. Num "606" see "atomic events provided by event sources 602"/As shown on figure 5, ref. Num "606" the atomic events are captured)* **the sensor located within an operating system kernel within a user client device;** *Column 28, lines 1-6 and column 22, lines 46-56* *[For instance on column 28, lines 1-6 the following has been disclosed. "In one embodiment, the HTTP client is implemented in kernel mode. Reasons for implementation in kernel mode include 1) performance; 2) communication with kernel components; and 3) listener/talker integration. The benefits of listener/talker integration include performance optimizations and shared implementation." Furthermore on column 22, lines 46-56 the following has been disclosed. The event system includes a highly optimized publication and subscription service driven by model-based subscription registrations. The events system allows for flexibility and choice of the service to publish events, such as, by way of example, kernel events (e.g. WDM drivers events) that utilize a kernel driver programming model, non-COM APIs for publishing events (e.g. security audit events, a directory, a service control manager) that utilize a low-level operating system service programming model, classic COM interfaces for normal*

applications, and high-level COM+ classes that utilize native COM+ programming model.) and

- a journaling server having **An aggregator, to accept or for accepting the atomic level events from the user client device and to generate an aggregate at least some of the atomic level events to generate at least one aggregate based on a predetermined sequence of atomic level events.** [column 21, lines 4-12 and column 20, lines 57-67] (*Event composition 608 aggregates, filters, and transforms lower-level events (atomic events 606) which meets the limitation of "multiple atomic level events" into higher-level events 612, which meets the limitation of a journal/aggregate event. And, at times, maps the events directly into actions, such as world action 614. The actions include real-world actions 614 and information-gathering actions 616 that serve to gather new events via actively polling or listening. **Event composition 608 provides methods for combining events** and data, whether the events are observed in close temporal proximity or at widely different times. On column 20, lines 57-67, the following has also been disclosed, "**The event component 155 transforms fundamental or atomic events 606 provided by event sources 602 into progressively higher-level events/predetermined sequence of atomic level; through an event composition mechanism 608.** The process of event composition is the construction of new events or actions from a set of observed events and/or stored event data. Event composition may be driven by rules, filters, and by more advanced pattern recognizers spanning a spectrum of sophistication all the way up to rich inferential machinery. Thus, event composition adapts the set of available atomic events 606 into observations 610 that are appropriately matched to the informational requirements of software components, providing them with information at the right level of abstraction to make good decisions.)*

Belfiore does not explicitly disclose, the following limitation added by the amendent.

"Having a reporter to generate an audit trail from the at least one aggregate event, the audit trail representing usage of the at least one digital asset by the end user"

However, in the same field of endeavor, **Ginter on column 65, lines 4-34** discloses the following which meets the above limitation.

"FIG. 35 shows an example overall usage clearing process. In this example, a provider 164 provides a digital property to consumers 95(1), 95(2), 95(3). For example, provider 164 might provide a novel or other work 166 to each of the consumers 95 within electronic containers 152. One or more control sets 188 may be associated with the work 166 (and may, in one example, be delivered within the same electronic container 152 used to deliver the work 166). The controls 188 may specify that certain types of usage information must be gathered in the form of an audit trail, and that the audit trail must be reported based on certain time and/or other events.

Because container 152 can only be opened within a secure protected processing environment 154 that is part of the virtual distribution environment described in the above-referenced Ginter et al. patent disclosure, provider 164 can be confident that the required audit trails will be generated and reported as he or she instructs. As consumers 95 use the property 166, their electronic appliances 100 automatically gather and store the usage information in the form of audit trails 302. Then, upon the occurrence of a specified event (e.g., once a month, once a week, after a certain number of uses, etc.), the consumer electronic appliances 100 send audit trail information 302 within digital containers to usage clearinghouse 300.

*Usage clearinghouse 300 collects the audit trail information 302, may store it in its database 316, and analyzes **the audit trail information to generate a report 304** which it may send to provider 164 within a further electronic container 152."*

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features such as "having a reporter to generate an audit trail from the at least one aggregate event, the audit trail representing usage of the at least one digital asset by the end user" as per teachings of **Ginter** into the method as taught by

Belfiore for the purpose of building a data security model which includes usage information while at the same time aggregating and providing a high level of accountability. [See for instance, Ginter column 57, lines 9-11]

6. **As per claims 2-3 the combination of Belfiore and Ginter discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system wherein, the aggregate events are associated with a particular executing process/with a particular user. [column 34-45 and column 21, lines 4-12 and column 20, lines 57-67] (The event component 155 of the present invention transparently facilitates the distributed communication of events between any software component that publishes or generates events ("event source") and any software component that subscribes to or receives event notifications ("event sink"). In this description and in the claims, an event is an observation about one or more states such as, for example, the status of system components, **the activity of a user.**)**

7. **As per claims 4 and 18 the combination of Belfiore and Ginter discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system wherein the user client device further includes: a filter for filtering atomic level events with an approved event list and wherein the aggregator only accepts atomic level events not filtered out by the filter. [Column 21, lines 4-19 and column 20, lines 62-column 21, lines 3 and column 22, lines 63-64] (Event composition 608 aggregates, filters, and transforms lower-level events (atomic events 606) into higher-level events 612 and, at times, maps the events directly into actions, such as world action 614. and on column lines it has been disclosed that Event composition may be driven by rules, filters, and by more advanced pattern recognizers spanning a spectrum of sophistication all the way up to rich inferential machinery. Thus, event composition adapts the set of available atomic events 606 into observations 610**

*that are appropriately matched to **the informational requirements of software components/ such requirements meets the limitation of approved event list,** providing them with information at the right level of abstraction to make good decisions.)*

8. **As per claims 5-6 and 19 the combination of Belfiore and Ginter discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system wherein the approved event list includes a list of approved file identifiers/hash code.***[Figure 5, ref. Num 610/612 and 622, column 21, lines 3-35] (As shown on figure 5, High level events shown as 612 which meets the limitation of approved event list is stored in event store as shown on figure 5, 622 inferences are performed. Such events should have some kinds of identifier when they are stored and hashing a value for the sake of utilizing the space requirement is something which is also included in storing the list of approved file identifiers /high level events 612)*

9. **As per claims 8 and 21 the combination of Belfiore and Ginter discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system** wherein the user client device includes: a coalescer to coalesce atomic multiple events output by the sensor into a single event prior to inputting them to the aggregator. *[Figure 5, ref. Num "606"]*

10. **As per claims 9-10 and 22 the combination of Belfiore and Ginter discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system wherein** a bundle of coalesced events is created prior to their transmission between the user client device and the server. *[Figure 5, ref. Num "608"/event composition meets the limitation of a bundle of coalesced events]*

11. **As per claim 11 the combination of Belfiore and Ginter discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system** wherein the at least one aggregate /journal event is detected as a

suspect action with a data file. [column 23, lines 64-column 24, lines 22 and column 21, lines 4-12 and column 20, lines 57-67]

12. **As per claim 12 the combination of Belfiore and Ginter discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system** wherein the at least one aggregate event is attributable to a known/end user, a thread and/or an application as identified at a known time. [figure 5, see "Time"]

13. **As per claim 13 the combination of Belfiore and Ginter discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system** wherein the coalescer reports a single coalesced event after a time out period with no activity. [column 24, lines 21-22, "notify me if there is no mouse movement and no key is pressed in 5 minutes")]

14. **As per claims 14-15 the combination of Belfiore and Ginter discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system wherein aggregate events are used to control security of the data processing system by determining patterns of unexpected behavior based on the at least one aggregate event and the audit trail.** [column 21, lines 50-53 and column 23, lines 64-column 24, lines 22 and column 21, lines 4-12 and column 20, lines 57-67, See also the following which is disclosed by Ginter on column 65, lines 4-34. "FIG. 35 shows an example overall usage clearing process. In this example, a provider 164 provides a digital property to consumers 95(1), 95(2), 95(3). For example, provider 164 might provide a novel or other work 166 to each of the consumers 95 within electronic containers 152. One or more control sets 188 may be associated with the work 166 (and may, in one example, be delivered within the same electronic container

152 used to deliver the work 166). The controls 188 may specify that certain types of usage information must be gathered in the form of an audit trail, and that the audit trail must be reported based on certain time and/or other events. Because container 152 can only be opened within a secure protected processing environment 154 that is part of the virtual distribution environment described in the above-referenced Ginter et al. patent disclosure, provider 164 can be confident that the required audit trails will be generated and reported as he or she instructs. As consumers 95 use the property 166, their electronic appliances 100 automatically gather and store the usage information in the form of audit trails 302. Then, upon the occurrence of a specified event (e.g., once a month, once a week, after a certain number of uses, etc.), the consumer electronic appliances 100 send audit trail information 302 within digital containers to usage clearinghouse 300. Usage clearinghouse 300 collects the audit trail information 302, may store it in its database 316, and analyzes **the audit trail information to generate a report 304** which it may send to provider 164 within a further electronic container 152.")

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4:30 pm).

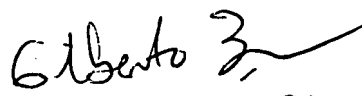
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax

phone number for the organization where this application or proceeding is assigned is 703-873-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.
11/22/2007


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100